

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA

**In the Matter of the Search of:**

Samsung Galaxy A30s Wireless Telephone,  
Seized from Timothy Woodruff, Jr.

Case No. 3:24-mj-00033

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Christopher A. Yarnell, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the seizure and forensic examination of the wireless telephone described in more detail in Attachment A hereto (the “TARGET DEVICE”) and the extraction from that wireless telephone the electronically stored information described in Attachment B hereto.

2. I am a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations (“HSI”). I have been so employed since June 2017. I am currently assigned to the Office of the Resident Agent in Charge HSI Charleston, West Virginia. I have experience in conducting investigations involving computers and the procedures that are necessary to retrieve, collect, and preserve electronic evidence. Through my training and experience, including on-the-job discussions with other law enforcement agents and cooperating suspects, I am familiar with the operational techniques and organizational structure of child pornography distribution networks and child pornography possessors and their use of computers and other media devices.

3. Prior to my employment with HSI, I was a Border Patrol Agent and a Task Force Officer (“TFO”) with HSI. I am a graduate of three federal law enforcement academies at the Federal Law Enforcement Training Centers (“FLETC”). I graduated from the United States Border Patrol Agent Academy in 2008, Criminal Investigator Training Program in 2017, and the Homeland Security Investigations Special Agent Training Program in 2018. As part of some of these programs, I received extensive training in the areas of law within the jurisdiction of HSI. I have specifically received training in the areas of child pornography and the sexual exploitation and abuse of children. This training includes specialized instruction on how to conduct criminal investigations related to violations of child protection laws pursuant to Title 18, United States Code, Sections 2251, 2252, 2252A, and 2256.

4. As a TFO, and later a Special Agent, with HSI, I worked at the office of the Assistant Special Agent in Charge in El Centro, California, where I investigated and assisted other law enforcement in federal and state criminal violations related to cybercrime, child exploitation, and child pornography. I have gained experience through training at FLETC, as well as on-the-job experience relating to investigations involving child exploitation offenses that occurred in the Southern District of California and the Southern District of West Virginia. I have received training, specifically Internet Crimes Against Children (“ICAC”) undercover chat training, in the areas of child pornography and child exploitation and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256(8)) in the form of computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251 (production of child pornography), 2252A(a)(1) (transportation of child pornography), 2252A(a)(2) (receipt or distribution of child pornography), and 2252A(a)(5)(B) (possession of child pornography), and I am authorized by

law to request a search warrant.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The probable cause statement is based upon information of which I am personally aware as well as information that has been conveyed to me by other law enforcement officers.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2251 (production of child pornography) and 18 U.S.C. § 2252A (transport, receipt, distribution, possession, and access with intent to view child pornography) (collectively, the “Subject Offenses”) have been committed by Timothy Woodruff Jr. (“WOODRUFF”). I seek to search the TARGET DEVICE to locate evidence of criminal violations of the Subject Offenses for items specified in Attachment B hereto.

#### **IDENTIFICATION OF THE TARGET DEVICE**

7. The property to be searched consists of a wireless telephone (i.e., the TARGET DEVICE), which is described in more detail in Attachment A hereto. The TARGET DEVICE was seized from WOODRUFF on or about April 27, 2022, and is currently in the possession of the West Virginia State Police (“WVSP”), Huntington Detachment, Huntington, Cabell County, West Virginia. Upon information and belief, the TARGET DEVICE is in substantially the same condition as it was on the date it was first seized.

8. The applied-for warrant would authorize the seizure and forensic examination of the TARGET DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.

### **DEFINITIONS**

9. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Computer: As defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
- d. Child pornography: As defined in 18 U.S.C. § 2256(8), means any visual depiction, including any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable form, that of a minor engaging in sexually explicit conduct; or such visual depiction has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

- e. Sexually explicit conduct. As defined in 18 U.S.C. § 2256(2)(A)(i-v), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person.
- f. Visual depiction. As defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disk or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

**BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, WIRELESS  
TELEPHONES, THE INTERNET, AND EMAIL**

10. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

11. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). Darkroom facilities and a significant amount of skills were required in order to develop and reproduce the photographic images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their detection by the public. The distribution of these wares was accomplished through a combination of personal contact, mailings, and telephone calls. Any reimbursement would follow these same paths.

12. The development of computers has added to the methods used by child pornography collectors to interact with and sexually exploit children. Computers serve four functions in connection with child pornography. These are production, communication, distribution, and storage.

13. Child pornographers can now transfer photographs from a camera in a computer-readable format. With the advent of digital cameras, the images can now be transferred directly onto a computer or wireless telephone. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through File Transfer Protocols to anyone with access to a computer or wireless telephone capable of Internet access. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “Instant Messaging”), and easy access to the Internet, computers and wireless telephones are preferred methods of distribution and receipt of child pornographic materials among pornographers.

14. A computer or wireless telephone’s ability to store images in digital form makes them ideal repositories for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers and other electronic devices such as cell phones or even gaming consoles has increased tremendously within the last several years. These drives can store hundreds of thousands of images at very high resolution.

15. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

16. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo!, Inc., and Google, Inc., among others. The online services allow a user to set up an account with remote access. Even in cases where online storage is used, however, evidence of child pornography can often be found on the user's computer or wireless telephone.

**CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS**

17. Based upon my knowledge, experience, and training in criminal investigations, particularly those that focus on child exploitation, as well as the training and experience of other law enforcement officers trained in child exploitation and child pornography investigations with whom I have had discussions, there are certain characteristics common to individuals involved in the possession, receipt and distribution of child pornography:

- a. Child pornography collectors may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- b. Collectors of child pornography may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Child pornography collectors often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce or to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Child pornography collectors typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.
- d. Likewise, collectors of child pornography often maintain their collections that are in a digital or electronic format in a safe, secure and private environment. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.



- e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.<sup>1</sup>
- f. Child pornography collectors also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- g. Collectors of child pornography prefer not to be without their child pornography for any prolonged time. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. It has long been recognized by professionals dealing with persons involved with child pornography that child pornography has enduring value to those involved in the sexual exploitation of children. Such persons rarely, if ever, dispose of their sexually explicit material. Those materials are often treated as prized possessions. Individuals involved in child pornography almost always maintain their materials in a place that they consider secure and where the materials are readily accessible. Most frequently, these materials are kept within the privacy and security of their own homes. These materials are often kept on their person in forms of media storage devices such as thumb drives and cellphones in their pants pockets and on their keychains.
- h. Further, it is common for such users to save and transfer the pornographic images and/or pornographic video of children from one computer to another because the images are generally difficult to obtain securely.

---

<sup>1</sup> See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).



18. Your Affiant believes that given the continuing nature of possession of child pornography and the general character of such offenders as “collectors” and “hoarders,” there is probable cause to believe that evidence of violations of federal law, including, but not limited to, 18 U.S.C. §§ 2252A(a)(2) (receipt or distribution of child pornography) and 2252A(a)(5)(B) (possession of child pornography) will be present on the TARGET DEVICE when the search is conducted.

**DETAILS OF THE INVESTIGATION/PROBABLE CAUSE**

19. On or about April 28, 2023, your Affiant received information from the United States Attorney’s Office for the Southern District of West Virginia that WOODRUFF had given a then-14-year-old minor male victim, whose identity is known to investigators but who shall be referred to herein as “MV1,” methamphetamine while MV1 was under his care and had shown MV1 pictures of himself (WOODRUFF) sexually abusing at least one other minor that WOODRUFF had stored on his wireless telephone. I was also informed that the Cabell County, West Virginia, Sheriff’s Office (“CCSO”) had investigated these allegations.

20. On or about May 2, 2023, I met with a CCSO deputy to discuss the details of the investigation regarding WOODRUFF and MV1. The deputy told me that WOODRUFF had previously provided methamphetamine to MV1, and MV1 had gone to school under the influence of methamphetamine. I later learned that WOODRUFF pled guilty on July 23, 2021, to contributing to the delinquency of a minor, in violation of West Virginia Code § 49-7-7, as a result of this incident.

21. Based on my conversations with the deputy and my review of reports prepared by CCSO, I learned the following:

- a. On or about April 18, 2022, MV1’s father contacted CCSO to report that WOODRUFF had sexually assaulted MV1 about a year prior by giving

MV1 methamphetamine and forcing MV1 to perform oral sex on WOODRUFF.

- b. On or about April 26, 2022, MV1 participated in a forensic interview at the Child Advocacy Center at Cabell-Huntington Hospital in Huntington, Cabell County, West Virginia. During the interview, MV1 disclosed that WOODRUFF had performed oral sex on MV1 approximately two or three times. After the formal interview had concluded, MV1 told the interviewer that WOODRUFF had shown MV1 a video of WOODRUFF having sex with another minor.
- c. WOODRUFF was under home confinement in April 2022 and was being supervised by CCSO home confinement officers. At the time, WOODRUFF resided in Kenova, Wayne County, West Virginia. On or about April 27, 2022, CCSO home confinement officers traveled to WOODRUFF's residence. Upon arriving, one of the officers searched WOODRUFF's cellphone (the TARGET DEVICE) pursuant to the Cabell County Alternative Sentencing Standard Terms and Conditions of Home Incarceration ("CHI"), which WOODRUFF had signed upon commencing his home confinement. The CHI WOODRUFF signed permitted an alternative sentencing officer ("ASO"), or any law enforcement officer designated by the ASO, to search, among other items, WOODRUFF's electronic communications devices to ensure compliance with the CHI.
- d. The home confinement officer who searched the TARGET DEVICE observed videos stored on the TARGET DEVICE that depicted WOODRUFF engaged in sexually explicit conduct with other individuals, but the officer was unable to confirm the ages of the other individuals depicted in the videos. WOODRUFF was also in possession of Neurontin<sup>2</sup> in an unmarked container and an excess of prescribed Suboxone<sup>3</sup> strips. WOODRUFF was arrested and transported to Western Regional Jail. The TARGET DEVICE was seized and turned over to a CCSO deputy.
- e. Because WOODRUFF resided in Wayne County, West Virginia, CCSO reported the findings of the investigation to WVSP for further investigation related to possible child pornography on the TARGET DEVICE. WVSP then took custody of the TARGET DEVICE.

---

<sup>2</sup> According to the website Drugs.com, Neurontin is the brand name for gabapentin, a prescription medication often used to treat nerve pain and seizures. Neurontin is a controlled substance under West Virginia law.

<sup>3</sup> According to the website Drugs.com, Suboxone is the brand name for a combination of buprenorphine and naloxone used to treat opiate addiction. Suboxone is a federal Schedule III controlled substance.

- f. The Cabell County, West Virginia, Prosecuting Attorney's Office declined to pursue charges against WOODRUFF for alleged sexual abuse of MV1 because WOODRUFF had already been prosecuted and pled guilty to contributing to the delinquency of a minor in connection with his conduct relating to MV1.

22. On or about July 12, 2023, your Affiant met with the CCSO home confinement officer who had searched the TARGET DEVICE on or about April 27, 2022. The officer informed me he observed about one hundred (100) videos of sexual acts on the TARGET DEVICE, some of which he believed involved minors. The officer explained that he believed some of the individuals depicted in the videos were minors because the individuals looked young, and their body parts were indicative of being younger than eighteen (18). The officer also told me that he thought WOODRUFF had two wireless telephones, but the officer was not sure. The officer provided me with a signed copy of WOODRUFF's CHI.

23. On or about July 21, 2023, I spoke to MV1's father. MV1's father indicated that he initially learned about what happened to MV1 because MV1's girlfriend had received messages from MV1 alleging that his babysitter had "messed around" with him. MV1's girlfriend told her mother about the messages, and the mother informed MV1's father. When MV1's father asked MV1 about the messages, MV1 told his father what had transpired with WOODRUFF. MV1's father indicated that MV1 was being cared for by WOODRUFF at the time of the alleged sexual assault and the methamphetamine usage in or around April 2021. MV1's father also said that MV1 had been doing better since learning that law enforcement was looking into MV1's allegations.

24. On or about July 25, 2023, I received a report detailing WVSP's investigation into this matter. The WVSP trooper who drafted the report wrote that she reviewed MV1's forensic interview conducted on or about April 26, 2022, during which MV1 recounted that he would

sometimes spend the night with WOODRUFF when MV1 was living with his mother, and WOODRUFF would “drug” MV1 by giving him methamphetamine or, on one occasion, Xanax, and then sexually “touch” him or give him “head” (which MV1 described as oral sex). MV1 stated that he had used methamphetamine with WOODRUFF approximately five (5) times. The trooper also spoke with the interviewer, who advised the trooper that after the interview concluded, MV1 stated that he had seen a video on WOODRUFF’s wireless telephone of what appeared to be WOODRUFF engaged in sexual intercourse with a minor. The trooper conducted a preview of the TARGET DEVICE and observed multiple videos of WOODRUFF engaged in sexually explicit conduct with others; however, the trooper did not observe any of the participants to be minors.

25. To date, neither CCSO nor WVSP has conducted a computer forensic review of the TARGET DEVICE. This search warrant seeks a computer forensic review of the TARGET DEVICE for evidence of violations of the Subject Offenses.

**SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER  
AND ELECTRONIC DEVICE SYSTEMS**

26. Based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers and other electronic devices, I know that data can be stored on a variety of computer systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage.

27. As is the case with most digital technology, communications by way of computer or wireless telephone can be saved or stored on the computer used for these purposes. Storing this

information can be intentional, i.e., by saving an e-mail as file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used.

28. I submit that there is probable cause to believe the items in Attachment B hereto will be stored on the TARGET DEVICE for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

29. As further described in Attachment B hereto, this application seeks permission to locate not only computer files that might serve as direct evidence of the Subject Offenses, but

also for forensic electronic evidence that establishes how the TARGET DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the TARGET DEVICE because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
- b. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatory or exculpatory the computer owner.
- d. Moreover, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner’s motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).
- e. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.



- f. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- g. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- h. I know that when an individual uses a computer to distribute or attempt to distribute child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of a crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

### **FORENSIC ANALYSIS**

30. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for would permit the examination of the TARGET DEVICE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the TARGET DEVICE to human inspection in order to determine whether it is evidence described by the warrant. If the TARGET DEVICE has been locked using a passcode, the examination may also include the use of computer programs or other devices to bypass the passcode or otherwise access the material located on the TARGET DEVICE.




CONCLUSION

26. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the TARGET DEVICE described in Attachment A to seek the items described in Attachment B.

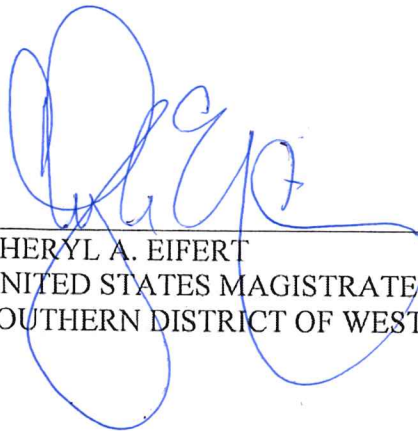
27. Moreover, I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, unless otherwise ordered by the Court, the return will not include the specific evidence later examined by a forensic analyst.

Further your Affiant sayeth naught.



SPECIAL AGENT CHRISTOPHER A. YARNELL  
DEPARTMENT OF HOMELAND SECURITY  
HOMELAND SECURITY INVESTIGATIONS

Sworn to before me this 4<sup>th</sup> day of June, 2024.



CHERYL A. EIFERT  
UNITED STATES MAGISTRATE JUDGE  
SOUTHERN DISTRICT OF WEST VIRGINIA